Софийски Университет „ Св. Климент Охридски”

Стопански факултет

Управленски Информационни Системи

**Курсова работа на тема:**

**Информационни системи: Защита и контрол**

**преподавател:**

ас. А. Антонова

**изготвил:**

**Ивалина Манчева, фн.78670**

гр. София, Февруари 2012 г.

Съдържание

[1. Въведение 3](#_Toc315907155)

[2. Теоритична част 4](#_Toc315907156)

[Уязвимост на системата и злоупотреба 4](#_Toc315907157)

[Информационна сигурност 5](#_Toc315907158)

[Физическа сигурност на компютърните системи 5](#_Toc315907159)

[Заплахи от собствения персонал 6](#_Toc315907160)

[Злонамерени действия от външни лица 7](#_Toc315907161)

[Phishing 8](#_Toc315907162)

[Вреден софтуер 8](#_Toc315907163)

[Kражба на самоличност 10](#_Toc315907164)

[Контрол на достъпа - автентикация 11](#_Toc315907165)

[3. Практически казус 15](#_Toc315907166)

[4. Заключения 22](#_Toc315907167)

[5. Референции 23](#_Toc315907168)

# Въведение

Информационните технологии навлязоха в много области на човешката дейност. Създават се различни информационни системи, предназначени за управление и общоползване от широк кръг потребители. Благодарение на Интернет информацията става все по-достъпна. Но това явление, освен че е полезно за много потребители, крие и много рискове в себе си.

Информацията е един от най-ценните ресурси във всяка инфраструктура, тъй като данните са градивният елемент, от който тръгва всеки процес, гради се услуга или продукт. Загубата на данни или разкриването на важна информация от недоброжелатели може да доведе до сериози загуби както за бизнеса, така и за всеки един човек по отделно. Основните видове заплахи за информационните системи могат да се разделят условно на заплахи от стихийни бедствия и аварии, сривове и откази на техническите средства на информационната система, последствия от грешки при проектиране и изработка на системата, грешки на персонала при работа със системата и преднамерени действия на нарушители и зложелатели.

Нито един от тези фактори не може да бъде предвиден със сигурност, а човешкият фактор и най-труден за преодоляване. Това, което всеки индивид или компания може да направи, е да не подценява риска и да вземе навременни мерки, за да защити информацията за себе си и да осиури неприкосновенността на личните данни.

# Теоритична част

## Уязвимост на системата и злоупотреба

Компютърните системи имат толкова важна и критична роля в бизнеса, правителството, и ежедневието, че фирмите трябва да направят сигурността и контрола свой основен приоритет. Сигурността се отнася до политиките, процедурите и техническите мерки, които се използват за предотвратяване на неразрешен достъп, промяна, кражба или физическо увреждане на информационните системи. Контролът се състои от всички методи, политики, и организационни процедури, които гарантират безопасността на организационните активи.

Информационните системи концентрират данните в компютърни файлове, които биха могли да бъдат достъпени от големи групи от хора в и извън организацията. Когато голямо количество данни се съхранява в електронна форма, данните стават уязвими към най-различни видове заплахи. Информационните системи в различни локации могат да бъдат свъразани чрез комуникационни мрежи, което увеличава риска от неоторизиран достъп, измами и злоупотреби, които могат да възникнат във вяка точка на мрежата.

Заплахите за съвременните информационни системи могат да произтичат от технически, организационни фактори, както и от фактори на околната среда, в допълнение с лоши управленски решения. В многослойна клиент-сървър компютърна среда, слабости съществуват на всяко едно ниво, както и в комуникацията между слоевете. Потребителите на клиентския слой могат да причинят вреда, чрез въвеждане на грешки или чрез достъп до системи без разрешение. Възможно е данните, предавани по мрежите, да бъдат достъпени, ценни данни да бъдат откраднати или съобщения да бъдат променяни без разрешение. Нарушителите могат да стартират атаки за отказ от обслужване или злонамерен софтуер, за да прекъснат функционирането на уеб сайтове. Тези, които могат да проникнат в корпоративни системи, могат да унищожат или да променят корпоративните данни, съхранявани в базите от данни или файлове.

На схемата долу са представени възможните заплахи на всяко едно ниво в средата и връзките между слоевете.



## Информационна сигурност

Информационната (компютърна) сигурност означава предпазване на информацията и информационните системи от неоторизиран достъп, употреба, запис, промяна, изтриване и т.н. Тя има три основни цели: да се запази поверителността, цялостта и наличността на информацията. Съществуват много и различни заплахи за информационната сигурност, с които компаниите се съобразяват.

### Физическа сигурност на компютърните системи

*Кражба или неоторизиран физически достъп*

Сървъри и дискови масиви с чувствителна информация трябва да са в сигурни и охранявани помещения. Много по-лесно е да се извади информация от сървър при физически достъп до него. Затова до тези помещения физически достъп трябва да има само минимален оторизиран персонал по поддръжка и охрана. Упражняват се контрол и наблюдение на достъпа.

*Природни стихии, технически сривове поради повреда или външни технически обстоятелства*

Съоръженията и компютърните системи трябва да бъдат добре подсигурени. Изграждат се противопожарни системи. Поддържат се подходящи условия – температура, вентилация, влажност. Обикновено за критични информационни системи, при които временното нарушаване на наличността на информацията носи големи загуби за компанията, се изграждат огледални системи, но на достатъчно географско разстояние. По този начин компаниите се предпазват от природни и други бедствия и повреди на компютърните системи – пожар, наводнение, липса на ток и т.н.

### Заплахи от собствения персонал

*Неволни технически грешки*

Една от най-сериозните заплахи за информационната сигурност са човешките грешки. Това е така, тъй като това е и най-често срещата причина за нарушаване на цялостта и наличността на информацията. Потребители и администратори допускат грешки, които водят до временна техническа неизправност на информационните системи, неволно инсталиране на вреден софтуер или загуба на информация. Защитата от такива грешки се осъществява чрез адекватно назначаване на минималните необходими права и възможности за използване на информационните системи, така че потребителите да могат да вършат своята работа. Така например, обикновено потребителите не могат да изтриват информация, създадена от други потребители. Различни технически обучения, процедури и правила за сигурна употреба спомагат за намаляването на такива грешки.

*Други грешки и социално инженерство*

Невежи потребители често не осъзнават важността на информационната сигурност. Често те записват своите пароли за достъп на хартия или я споделят с колеги. Недоброжелатели се възползват от необучени потребители и се представят за технически персонал в опит да получат пароли или други конфеденциални технически детайли. За избягването на тези проблеми е необходимо да се запознаят потребителите на информационните системи с рисковете, както и да има ясни правила и процедури за употреба.

*Злонамерени служители*

Обикновено това е най-лесният начин за изнасяне на конфеденциална информация от компанията. Затова трябва да се спазва правилото за минимално възможен достъп до информация, който е достатъчен за работата на служителите. Въпреки това, такава заплаха съществува от технически персонал, ръководен персонал, служители по сигурността. Такива потребители често имат информация за технически детайли на информационните системи. Могат да практикуват и социално инженерство върху други служители.

### Злонамерени действия от външни лица

Съществуват различни категории хора, които се занимават с неоторизиран достъп. Целите им също са различни: индустриален шпионаж, нелоялна конкуренция, финансови облаги, отмъщение, вандализъм и др. При такива пробиви не винаги има разрушение на информация, а понякога компанията не разбира, че е изтекла информация.

*Хакери и кракери*

В литературата се прави разлика между хакер, което означава високо квалифициран и добронамерен компютърен специалист и кракер - това е хакер, който използва своите способности с користна цел. Обикновено до неоторизиран достъп се стига след предварително проучване, социално инженерство и др. Чрез продължително следене се изгражда профил на системите за сигурност и нейните пропуски.

*Неоторизиран достъп чрез пароли*

Съществуват списъци с често използвани пароли. Недоброжелатели могат да използват тези списъци за да атакуват потребителски акаунти, които имат права и привилегии върху чувствителни информационни системи. За да се избегне тази опасност се въвеждат стандартни изисквания към паролите – например минимална дължина, наличие на цифри и специални символи.

Някои кракери използват програми, които генерират милиони възможни пароли в секунда. В някои случаи, при достатъчно кратки пароли се опитват всички възможни коомбинации до намиране на правилната парола. За неутрализиране на тази заплаха основно значение имат отново гореспоменатите изисквания към паролите за сложност и минимална дължина, както и така нареченото „заключване“ на акаунт след въвеждане на определен брой грешни пароли за малък период от време. Още по-сигурно решение е въвеждането на двуфакторна автентикация чрез използване на цифрови сертификати или RSA SecurID.

### Phishing

Представлява мрежова заплаха, при която чрез достъп до мрежов ресурс се следи трафика, който минава през него. Това е опасно и често може да остане незабелязано. При някои по-стари системи дори потребителски пароли се предават в прост текст и чрез този метод лесно могат да бъдат записани от зложелатели. За избягването на тази заплаха трябва да се подсигури мрежовото оборудване в компанията, а обменянето на чувствителна информация с потребители в Интернет трябва да бъде криптирано. Това може да стане например чрез използване на VPN връзки и/или цифрови сертификати.

### Вреден софтуер

Съществуват различни видове вреден софтуер. Общото за него е, че обикновено се инсталира без знанието и съгласието на потребителя и има за цел да предостави или компрометира по някакъв начин информационната система.

*Шпионски софтуер (Spyware)*

Следят и записват информация за използването на компютъра. Следят се навиците на потребителите и спомагат за разучаването на хакери. Информацияте се предава до определен получател.

*Логически бомби*

Стар тип зловреден софтуер. Обикновено не въздействат на системата по никакъв начин докато не се изпълни определено условие. След изпълнение са разрушителни.

*Троянски коне*

Инсталират се в допълнение към полезни програми и дават достъп до комптърната система на определени зложелатели. Определени хора могат да достъпват ресурси в заразената система избягвайки стандартните системи за сигурност. Могат да се изпълняват различни команди, да се прехвърлят файлове и друга информация, да се управлява компютърната система. За разлика от традиционните вируси, тези програми не заразяват други файлове.

*Червеи*

Тяхната основна цел е да се разпространяват в други системи чрез използване на достъпни мрежови връзки. Понякога се разпространява и чрез електронна поща. Може да носи и разпространява друг вреден софтуер.

*Вируси*

Представляват програми, които записват части от себе си в легитимни, полезни програми. Всяко тяхно копие след това може отново да се разпространява в други достъпни програми. Освен разпространението им, те обикновено имат и разрушително или друго вредно действие. Обикновено развитието на вирусите протича на етапи, така че те не изпълняват същинската си цел преди да е свършила тяхната фаза на разпространение. Някои от основните видове вируси са:

* Заразяващи изпълними програмни файлове (\*.exe, \*.dll, \*.sys и т.н.). Някои са полиморфни, т.е. променят кода си при разпространение в опит да не бъдат идентифицирани от антивирусните програми;
* Заразяващи системни или boot записи. Обикновено променят части от паметта на компютъра, които се четат преди зареждане на операционната система. Много разрушителни;
* Невидими вируси – те са специално проектирани така, че да не бъдат открити от антивирусния софтуер. Те скриват измененията, направени от тях в заразените файлове чрез контролиране на системните функции на операционната система и антивирусната програма.

Съвременните антивирусни решения имат два основни модула – сканиращ и предпазващ.

Чрез сканиращия модул, потребителят може да открива и премахва вируси при проверки, инициирани от него. Използват се бази данни с кодове на известни вируси, както и интелигентни системи, които анализират изпълнимите файлове и могат с голяма точност да ‚предположат‘ наличието на вреден софтуер.

Предпазващият модул се зарежда в паметта при зареждане на операционната система. Той наблюдава всички процеси и анализира тяхното поведение. Той има превантивна функция, тъй като е трудно вирус да зарази системата без да бъде забелязан.

### Kражба на самоличност

С разрастването на Интернет и електронната търговия, кражбата на самоличност става особено тревожна. Кражбата на идентичност е престъпление, в което измамник получава ключови части от лична информация, като ЕГН, номер на шофьорска книжка или номера на кредитни карти, за да се представи за някой друг. Информацията може да се използва за получаване на кредит, стоки или услуги, в името на жертвата, или за предоставяне фалшиви идентификационни данни на крадеца.

Интернет улеснява крадците на идентичност при използването на открадната информация, тъй като стоки може да бъдат поръчани онлайн без някаква лична намеса. Файловете за кредитни карти са основната цел на хакерите. Сайтовете за електронна търговия са прекрасни източници на лична информация за клиентите: име, адрес и телефонен номер. Разполагайки с тази информация, престъпниците маогат да приемат нова идентичност и да създадт нови кредити за собствените си цели.

„Фишингът“ става все по-популярна тактика за измама. Създават се фалшиви уеб сайтове или се изпращат e-mail съобщения, които изглеждат като тези на законни компании. Те изискват от потребителите поверителни лични данни. Съобщение в e-maila инструктира получателите да актуализират или да потвърдят данни чрез предоставяне на ЕГН (личен идентификационен номер), информация за банкови сметки и кредитни карти, както и други поверителни данни. Потребителят прави това или чрез отговор на е-мейл-а, или чрез въвеждане на желаната информация на фалшив уеб сайт.

## Контрол на достъпа - автентикация

Контролът на достъпа се състои от всички политики и процедури, които една компания използва, за се предотврати незаконен достъп до системите от неоторизирани външни и вътрешни лица. За да получи достъп потребителят трябва да бъде оторизиран и автентициран.

Автентикация е термин, който означава проверка на принадлежността на субекта към предявения от него идентификатор или потвърждение за автентичност. Един от начините за автентикация на потребител пред компютърна система - например операционна система — е да въведе идентификатор, например име на потребител и парола — които разрешават ползването на определен ресурс. След като получи от потребителя въведеното потребителско име и парола, компютърът ги сравнява със стойностите, които се съхраняват в специална база от данни и ако съвпадат, допуска потребителя в системата. Самата парола се явява гарант че потребителя или устройството са автентични. При всяка следваща употреба, потребителят трябва да знае и ползва по-рано обявената парола. Слабост на тази система е че потребителите често забравят своите пароли, споделят ги или избират пароли, които лесно биха могли да бъдат отгатнати. Всичко това излага на риск сигурността.

Малките и средни предприя (МСП) автентицират своите крайни потребители предимно с пароли, въпреки че паролите са по-несигурни, неудобни и фактически по-скъпи от някои по-надеждни форми на автентикация. В сравнение с по-големите организации МСП харчат средно 38% по-малко за идентифициране и автентикация на потребителя. Но това е неправилно решение, тъй като те понасят 87% повече разходи за всеки потребител, поради инциденти, свързани със сигурността. Установено е, че надеждните решения за автентикация, които обикновено са добре проектирани, за да отговорят на нуждите на МСП, включват евристична/адаптивна/базирана на риска автентикация, телефонна автентикация и верификация и многофункционални смарт-карти. През 2011 много предприятия започват активно преоценяване на стратегиите си за автентикация на крайните потребители.

**Паролите не са толкова сигурни:**

Според проучване на Aberdeen Group, направено сред група организации за период от 12 месеца, инцидентите при тези компании, използваща пароли, са с 5% повече от тези с по-надеждни методи за автентикаци. Такива инциденти са неупълномощен достъп до ресурси, загуба на данни.

**Паролите са неудобни:**

Голяма част от предприятията вземат мерки за усилване на сигурността на традиционните пароли, например:

- изисквания за дължина (87%), сложност (80%), честота на промяна (85%) и ограничения за повторно използване (84%)

- изключване на стандартни термини (53%)

Всички тези стъпки усилват надеждността на паролите, като ги правят по-трудни за отгатване, но в същото време ги правят по-тромави и трудни за запомняне от крайните потребители.

**Паролите са по-скъпи:**

Приблизителната оценка на годишните разходи за управление на идентификация и автентикация - включително всички служители, процеси, технология, хардуер, софтуер, услуги, обучение и поддръжка, възлизат на $12.60 за групата, използваща по-надежни методи на автентикация, и $13.70 за тази, използваща пароли. В крайна сметка, групата от предприятия, използваща по-силна автентикация, показва по-добра ефективност (по-ниски общи годишни разходи за краен потребител) и по-добра ефикастност (по-малко на брой годишни инциденти, свързани със сигурността). МСП в момента изпозват предимно пароли за автентикация на своите потребители, но много от тях планират в рамките на 12 месеца да въведат по-надеждни методи. Най-висок интерес на пазара будят:

- адаптивна автентикация - наблюдават и анализират онлайн дейностите на потребителите в реално време, за да генерират оценка за гарантиране на идентичността, базирана на риска. За да се определи дали потребителско име и парола са достатъчни за автентикация за съответната транзакция, се използва корелация на информацията относно устройствата, поведението на потребителите, данни от външни наблюдаващи устройства.

- смарт карти - обикновено се използват с дигитални сертификати. Те са многофукционални, като могат да се използват в редица случаи, като автентикация (например за компютър, достъп до мрежата, отдалечен достъп, за привилигировани администраторски акаунти), подписи (например за e-mail), криптиране на чувствителни, данни (e-mail, таен трансфер на данни), вход в сгради (интегрирани със системи за контрол на физическия достъп), фото-идентификация.

- телефонна автентикация - потребителите въвеждат потребителското си име и парола на някой уеб сайт, след което получват телефонно обаждане или sms като допълнителна неразделна част от процеса на автентикация.

- биометричната автентикация- обещаваща технология, която може да преодолее някои от недостатъците и ораниченията на паролите, като начин за автентикация на потребителите. Биометричната автентикация се базира на измерване на физически или поведенчески черти, които правят потребителя уникален. Тя сравнява уникални личностни характеристики, като пръстов отпечатък, лице, ретина, с определен съранен профил на тези характеристики. Така се определя дали има някакви различия между двете. Достъпът е осигурен, ако двата профила съвпаднат.



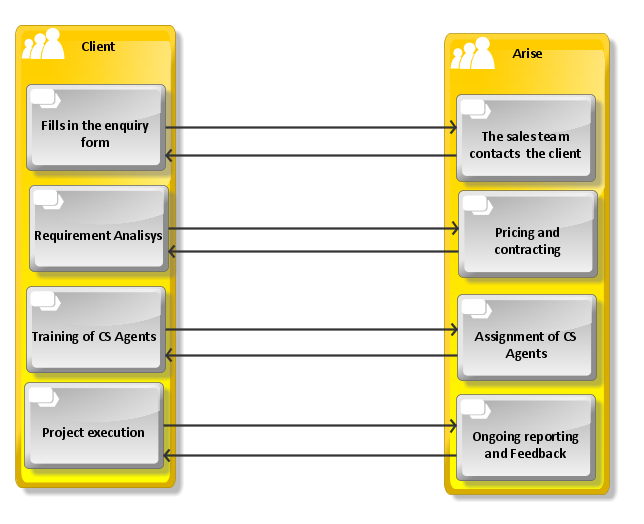
# Практически казус

Arise Solutions Incorporated e oснована през 1997 г. в Мирамар, Флорида. Тя е водещ в света доставчик на виртуални бизнес услуги за марки, които се опитват да подобрят бизнес резултатите си чрез своите продажби и канали за обслужване. Arise Solutions предлага висококачествено обслужване на клиентите по телефона, електронната поща или чат, техническа поддръжка и продажби чрез мрежа от самостоятелни професионалисти, работещи от вкъщи. Уменията на Професионалистите, сертифицирани от Arise, отговарят на целите на клиентите на компанията и нуждите на техните потребители.

**Ключови изисквания**

Arise Virtual Solutions предоставя виртуални кол център услуги на някои от най-престижните компании в света. Обхващайки отрасли като търговия на дребно, транспортната индустрия и компютърните технологии, Arise управлява над 8000 бизнес партньори, които служат като представители в кол центрове и всички работят от отдалечени места.

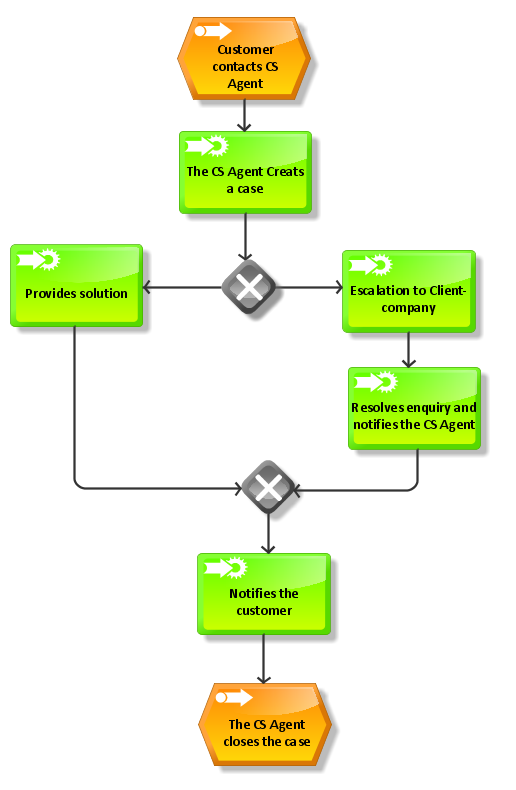
На Фиг.1. „Business view“ е преставен процесът на сключване на договор между Arise и компания-клиент. Клиентът желае да използва услугите на Arise, която да предоставя висококачествено обслужване потребителите на компанията-клиент. Клиентът попълва формуляр със запитване и го изпраща по електронната поща. Представител на Arise се свързва с клиента по телефона или му изпраща e-mail с отговора. Необходимо е клиентът да направи анализ на изискванията си относно облужването и да и представи на Arise. Въз основа на това се определя цената на услуата и се създава договор с необходимите условия. Подписва се и Service Level Agreement (SLA), в който са описани задълженията на Arise по отношение на обслужването, като например време, за което трябва да е разрешен един проблем или да е обслужен даден потребител. Arise определя кои от сертифицираните професионалисти са най-подходящи за този проект, след което те биват обучени от компанията-клиент. След стартирането на проекта, Arise следи качеството на предлаганите услуги и периодично уведомява клиента си за това.



*Фиг.1. Business view*

Тъй като много от техните клиенти се обаждат за лична информация, например данни на кредитна карта, Arise е длъжна да се съобразява със стандартите на Payment Card Industry(PCI), за да може да събира такава информация по телефона. Тъй като те служат като виртуален кол център, PCI стандартът изисква двуфакторно удостоверяване на всеки, който достъпва данните от разстояние. За да отговори на нуждите на своите клиенти и да се съобрази с PCI, Arise изисква надеждна двуфакторна автентификация за техните бизнес партньори. С такава голяма дистанционна потребителска база, те търсят решение, което би било лесно за управление и използване.

На Фиг.2. „Process View“ е показан процесът на обслужване на краен потребител. Потребителят установява контакт с представител на отдела за поддръжка, като обяснява своя проблем или прави запитване. Операторът регистрира проблем в системата. За тази цел е необходимо той да има оторизиран достъп до системата на компанията-клиент. Ако операторът може да разреши проблема или да даде нужната информация, той я предоставя на потребителя и записва това в системата. В случай на необходимост, проблемът се прехвъля към компанията-клиент и цлед разрешаването му, операторът информира крайния потребител. Тъй като се работи с лични данни и конфиденциална информация, е необходимо агентът да бъде автентициран, за да получи достъп до системата и базата от данни на компанията-потребител. От друга страна и крайният потребител също трябва да се идентифицира по някакъв начин пред агента. Само собственикът може да получи информация за своя акаунт.

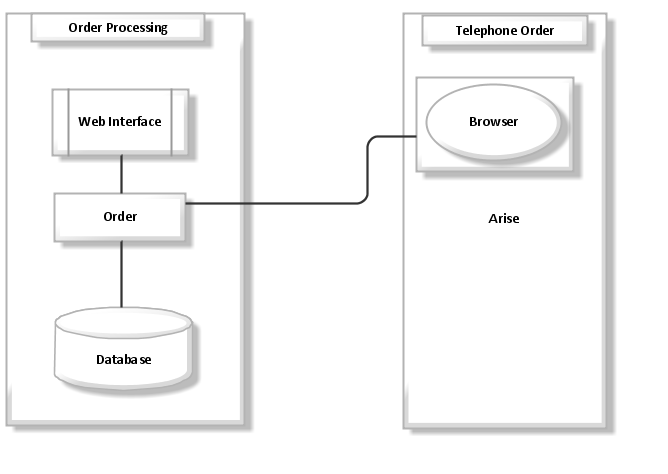


*Фиг.2. Process view*

**Решение**

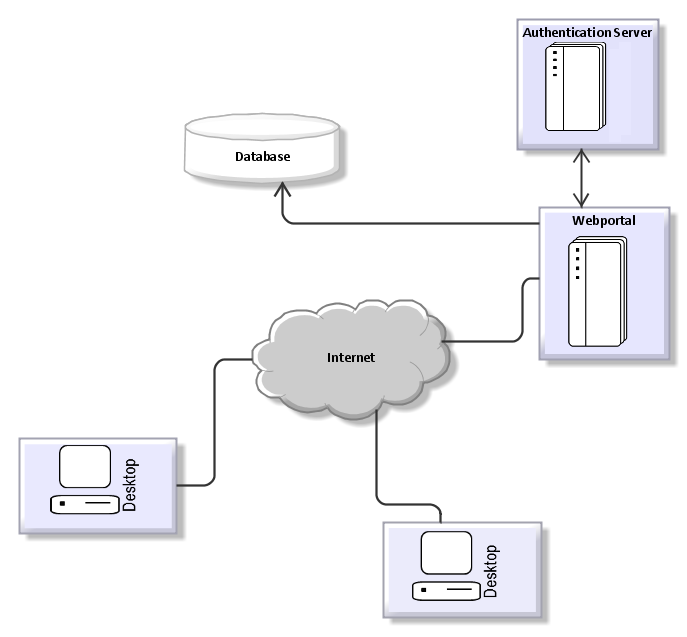
Преди да направи окончателното си решение Arise оценява няколко решения за двуфакторна автентикация. Другите решения не предлагат достатъчно гъвкав вътрешен контрол и системна интерация. В края на краищата Arise избира решението на RSA SecurID, защото то е лесно за управление и би могло лесно да се интегрира в съществуващата IT инфраструктура на компанята. Решението е оперативно съвместимо с повече от 350 приложения от трета страна и предлага опции за удостоверяване с еднократна парола, включително софтуер, хардуер и SMS опции. С голямата си потребителска база Arise са наясно с предизвикателствата, които могат да възникнат при прилагане на нова технология. За да сведат проблемите до минимум, те решават да започнат с постепенно въвеждане на крайните потребители. Въздействието върху работния процес е сведено до минимум и в рамките на две седмици след като въвеждането е завършено, всички от първоначалните им проблеми с поддръжката са решени. По-късно Arise решава да премине към използване на софтуерни автентикатори за защита на отдалечения достъп. През септември 2008 г., те започват да предлагане RSA SecurID Token за Windows-базирани работни станции. След като тригодишният живот на хардуерните автентикатори е изтекъл, бизнес партньорите трябва да изтеглят SecurID Desktop Software Token. Има две основни причини, поради които Arise избира софтуерния автентикатор. Първо, така ще се намалят общите разходи, тъй като софтуерните автентикатори могат да се използват многократно и не могат да бъдат изгубени. Така, Arise няма да се тревожи, че ще изгуби token, ако някой партньор напусне компанията, тъй като софтуерния автентикатор може бързо и надеждно да пъде преназначен на друг потребител. Второ, постоянното администрарене и подменяне на хардуерни автентикатори за около 8000 отдалечени потребителя, изисква персонал и ресурси. С преминаването към софтуерни автеникатори тази административна работа не е необходима. Назначаването им става само чрез изпращане на линк за изтегляне.

На фигурата по-долу изобразява примерен модел на регистриране на телефонна поръчка. Агент на Arise чрез браузър достъпва уеб-базиран интерфейс на клиента и подава своята заявка към базата данни. RSA осигурява многофакторно удостоверяване. Продуктът позволява да се осигури защитен достъп до информация на отдалечените служители, като същевременно се гарантира тяхната идентичност.



*Фиг.3. Application view*

Схемата по-долу посочва как технически са разпределени процесите. Отдалечените агенти на Arise през Интернет се свъзват с уеб-портала на компанията клиент, като те трябва да се автентицират пред него за да получат достъп. Чрез използване на RSA-продукта Arise защитава SSL VPN мрежите и уеб-порталите срещу неоторизиран достъп. Тази технология осигурява автентификация, която е съобразена с изискванията за сигурност. След като служителят въведе своя PIN и 6-цифрен „token“ код, уеб порталът сравнява информацията с тази от Authentication сървъра и ако тя съвпада, разрешава достъпът до базата данни. По-нататък връзката между агента и базата от данни се осъществява само през уеб-портала, без участието на автенификационния сървър.



*Фиг.4. Technical view*

**Резултати**

Arise използва надеждна двуфакторна автентикация, за да защитава Citrix и други приложения на своите клиенти. За да може бизнес партньор от отдалечена локация да достъпи системите на клиента и да отговори на обаждане от тяхно име, той трябва да бъде автентициран. Потребителите просто комбинират таен Личен Идентификационен Номер (PIN) в 6-цифрения код, който се появява на екрана на автентикатора им в съответното време. 6-цифреният код се променя на всеки 60 секунди, което го прави много сложно за заобикаляне. Резултатът е уникална еднократна парола, която осигурява надеждна двуфакторна автентикация на потребителя. Потребителят получава достъп до защитените ресурси, след като кодът бъде валидиран. Чрез използване на водещата технология за автентикация, Arise успява да отговори на изискванията на своите клиенти. За Arise това означава да предложи двуфакторна автентикация на всичките си бизнес партньори, които работят от различни места. Сертификатът от PCI дава на Arise предимство пред потенциални нови клиенти, тъй като това е ключов фактор за корпорации, които искат да изнесат техните операции с поддръжката на клиенти. В допълнение, Arise демонстрира огромно внимание върху сигурността на приложенията и данните на своите клиенти.

# Заключения

Макар може би и недооценени, сигурността и контролът са станали критична област за инвестиция в информационните системи. Когато компютърните системи не могат да работят или не работят според изискванията, фирмите, които са силно зависими от компютрите, търпят сериозни загуби. Колкото по-дълго компютърните системи не работят, толкова по-сериозни са последствията за фирмата. И с толкова много работа, която сега зависи от Интернет и мрежовите системи, фирмите са по-уязвими от всякога от нарушаване и вреди.

Компаниите разполагат с много ценни информационни активи на информация, които трябва да защитават. Системите често пазят поверителна информация за данъците на физическите лица, финансови активи, медицински досиета. Те също могат да съдържат информация за корпоративната дейност, включително търговски тайни, планове за разработка на нови продукти, както и маркетингови стратегии. Държавните системи могат да съхраняват информация за оръжейни системи, разузнавателни операции и военни цели. Тези информационни активи имат огромна стойност и ако те бъдат изгубени, унищожени или попаднат в неподходящи ръце, последиците могат да бъдат опустошителни.

В дигиталния свят данните представляват нещо повече от битове, записани на устройството за съхранение. Те са продукт на часове интелектуални усилия и упорита работа; ценна информация, която е от жизненоважно значение за вашия бизнес или фирма. За съжаление, загубата на данни е често срещано явление и може да доведе до загуба и на усилия, и на пари.

Недостатъчната сигурност и контрол, също могат да създадат сериозни законови спънки. Бизнесът трябва да защитава не само собствените си информационни активи, но също така и тези на клиенти, служители и бизнес партньори. Неспособността да направи това може да доведе фирмата до скъпоструващи съдебни спорове за излагане или кражба на данни. Всяка организация трябва да оцени рисковете и да вземе навреме съответните защитни действия за предотвратяване на загубата на поверителна информация или нарушаване правото на неприкосновеност на личните данни.

# Референции

1. Laudon, К. & Laudon, J. (2007). *Management Information Systems.* Prentice Hall.
2. Markus Hanhisalo. *COMPUTER VIRUSES:*

<http://www.tml.tkk.fi/Opinnot/Tik-110.501/1997/viruses.html#2.1.1> , 29.01.2012

1. Aberdeen Group

<http://www.rsa.com/products/AMX/pdfs/11607_0268-XXXX-SI-SMB-DBLH-06-vF.pdf> , 30.01.2012

1. Arise Virtual Solutions, [www.RSA.com](http://www.RSA.com)

<http://www.rsa.com/products/securid/success/9801_ARISE_CP_0611.pdf> , 28.01.2012